



Department of Homeland Security Daily Open Source Infrastructure Report for 07 August 2006

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports that in the past 18 months, colleges were the source of one-third to one-half of all publicly disclosed cybersecurity breaches, which is a larger share than the financial services, government, retail, or health care sectors. (See item [8](#))
- The U.S. Food and Drug Administration Center for Toxicological Research is developing a quick, cost-effective method using mass spectrometry to screen for and identify bioterror agents and other substances used in hoax incidents. (See item [23](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. **August 03, U.S. Department of Energy** — **DOE continues path forward on Global Nuclear Energy Partnership.** The U.S. Department of Energy (DOE) Thursday, August 3, announced \$20 million to conduct detailed siting studies for public or commercial entities interested in hosting DOE's Global Nuclear Energy Partnership (GNEP) facilities. Entities could qualify to receive up to \$5 million per site. GNEP, launched earlier this year as part of the President's Advanced Energy Initiative, aims to expand the use of nuclear energy to address the growing demand for energy. GNEP proposes private-public-international partnerships to develop advanced technologies to recycle used nuclear fuel, reduce wastes, and avoid misuse of nuclear

materials.

The Financial Assistance Funding Opportunity Announcement may be found at:

<http://gnep.gov/>.

Source: <http://www.doe.gov/news/3884.htm>

- 2. August 03, WTOL (OH) — Smoldering embers cause for alarm at Consumer's Energy power plant.** Some smoldering embers were the cause for alarm on Thursday morning, August 3, at the Consumer's Energy power plant in Luna Pier, MI. Fire crews were called to the J.R. Whiting Power Plant just after 10:00 am CDT after crews at the plant found embers smoldering under a conveyor belt. The conveyor belt carries coal from stockpiles into the plant. The plant's own fire department started dousing the embers, but called in four local fire companies as backup. There was no affect on operations.

Source: <http://www.wtol.com/Global/story.asp?S=5235757>

- 3. August 03, Reuters — Thousands of customers without power in Ontario, Quebec.** More than 210,000 electricity customers in Ontario and Quebec were without power on Thursday, August 3, after a series of violent thunderstorms over the past couple of days. The storms on Wednesday night left some 120,000 customers out across Hydro One's service area in Ontario. Hydro-Quebec was still working to restore service to about 94,000 customers in Quebec who lost power due to Tuesday night storms. After a heat wave blanketed the region this week, boosting Ontario's power usage to record levels, officials at both utilities said the outages were related to the storms, not the heat. Quebec, which uses electricity for heating, sees power demand peak in the winter. At its worst, more than 462,000 Hydro-Quebec customers were in the dark Tuesday night, August 1.

Source: http://ca.today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006-08-03T181811Z_01_N03129794_RTRIDST_0_CA_NADA-UTILITIES-HYDROQUEBEC-OUTAGES-COL.XML

- 4. August 03, Associated Press — Lightning strikes power plant in central Wisconsin.** Lightning struck Weston 3, one of several coal-fired units at the Weston plant near Wausau, WI, Wednesday, August 2, prompting Wisconsin Public Service Corp. (WPS) to ask customers in north-central and northern Wisconsin to conserve electricity. Also, a separate coal unit there is out of service because of a small coal fire in that unit's pulverizer, WPS said. That fire was contained and nobody was hurt, and that unit is expected to return to service Thursday. The utility has interrupted service to large commercial industrial customers in the area.

Source: http://www.gazetteextra.com/powerplant_lightning080306.asp

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *August 03, GovExec* — **IG recommends early contracting personnel involvement in reconstruction.** A special inspector general (IG) for Iraq's reconstruction advised that agencies consider developing a set of contracting rules for use in defense contingencies and that they involve purchasing personnel earlier in predeployment planning, among other measures. In a report on lessons learned in contracting and procurement, Special Inspector General for Iraq Reconstruction Stuart Bowen emphasized that agencies should involve procurement personnel in all planning stages; clearly define and communicate procurement roles and responsibilities for cooperating agencies, emphasize contracting support for small, easily executed projects in the early reconstruction phases that can quickly meet immediate needs; and avoid using sole-source and limited competition contracting strategies that hurt transparency. IG report: http://www.sigir.mil/reports/pdf/Lessons_Learned_July21.pdf
Source: http://www.govexec.com/story_page.cfm?articleid=34704&dcn=to_daysnews

[\[Return to top\]](#)

Banking and Finance Sector

6. *August 03, ATM Marketplace* — **Japan limits cash transfers at ATMs.** In a bid to combat money laundering and terrorist financing, Japan's Financial Services Agency (FSA) will limit cash transfers from ATMs to 100,000 yen (U.S. \$869) per transaction. The limit, which is currently two million yen, on January 4, 2007, will be reduced for remittances made at foreign ATMs; a customer can still transfer up to two million yen, if he uses an ATM operated by a financial institution he banks with. The move is part of FSA's push for financial institutions to implement stricter standards to verify customers' identities at bank counters, officials said. Source: http://www.atmmarketplace.com/research.htm?article_id=26380&pavilion=24&step=story
7. *August 03, Register (UK)* — **eBay scamming automation primed for fraud.** Scammers are starting to use automated bots in a bid to establish a bogus eBay reputation that will later allow them to dupe gullible users through bogus auctions. By automating the process of creating an account with an ostensibly good reputation, crooks can avoid the tedious business of building up a decent profile before looking to cash in with a scam auction. The "eBay scamming automation" begins with the creation of randomly named, fake user accounts. These fake users, powered by automated Web spider software, search eBay for extremely low value "buy it now" items, such as eBook or wallpapers, and place a purchase. As Fortinet points out, most one-cent-plus-no-delivery-cost sellers automate the whole transaction: should someone buy their eBooks, a script e-mails it automatically to the buyer, and leaves a standard feedback comment on the buyer's profile. The fake user then automatically responds with a standard feedback comment on the seller's profile. Software bots talk to software bots, and scammers can build up multiple fake accounts. Source: http://www.channelregister.co.uk/2006/08/03/ebay_scam_automation/
8. *August 03, Associated Press* — **Colleges are textbook cases of cybersecurity breaches.** A growing concern among privacy advocates: College and universities aren't up to speed when it comes to safeguarding information on their networks. In the past 18 months, colleges were the source of one-third to half of all publicly disclosed breaches, which is a larger share than financial services, government, retail, or health care. Privacy advocates say the breaches come

at a time when higher education is under growing pressure to collect data on students. Recently, a federally appointed commission proposed that the Department of Education maintain a system to report personal, financial, and academic data for every college student. No federal laws require businesses, non-profits, or public institutions to notify consumers when personal information has been compromised. Thirty-four states require such notification. Linda Foley of the Identity Theft Resource Center says colleges may be more likely than businesses to report network breaches. Also, unlike most businesses, which usually have a clear chain of command, campuses typically are decentralized. That makes it harder to ensure adequate security measures are in place across the board.

Source: <http://www.stevenspointjournal.com/apps/pbcs.dll/article?AID=/20060803/SPJ0101/608030366&template=printart>

[\[Return to top\]](#)

Transportation and Border Security Sector

9. *August 04, Government Accountability Office* — **GAO-06-1027T: Gas Pipeline Safety: Views on Proposed Legislation to Reauthorize Pipeline Safety Provisions (Testimony)**. The Pipeline Safety Improvement Act of 2002 established a risk-based program for gas transmission pipelines—termed integrity management—which requires pipeline operators to identify areas where the consequences of a pipeline incident would be the greatest, such as highly populated areas. Operators must assess pipelines in these areas for safety threats (such as corrosion), repair or replace defective segments, and reassess their pipelines at least every seven years. Under the Pipeline and Hazardous Materials Safety Administration's (PHMSA) regulations, operators must reassess their pipelines for corrosion at least every seven years and for all safety threats at least every 10, 15, or 20 years. State pipeline safety agencies that assist PHMSA are eligible to receive matching funds up to 50 percent of the cost of their pipeline safety programs. This statement is based on ongoing work for this Subcommittee and for others. It focuses on three areas germane to current legislative reauthorization proposals: (1) an overall assessment of the integrity management program, (2) the seven-year reassessment requirement, and (3) provisions to increase state pipeline safety grants. The Government Accountability Office contacted more than 50 pipeline operators and a broad range of stakeholders and surveyed state pipeline agencies.

Highlights: <http://www.gao.gov/highlights/d061027thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-1027T>

10. *August 04, USA TODAY* — **More air passengers getting bumped**. Airline passengers in the U.S. are getting bumped off flights more frequently than at any time in the last six years, the government reported Thursday, August 3. Some 16,300 passengers were bumped against their wishes in the April-June quarter, a rate of 1.12 passengers per 10,000. That rate is one-third higher than a year earlier. The airlines' rate of what the Department of Transportation (DOT) calls "involuntary denied boardings" was the highest since the same quarter in 2000. In all, the DOT said, airlines bumped about 185,000 passengers during the last quarter, also up from the year-ago quarter. Most volunteered to give up their seats. The worsening problem with bumping reflects the intensifying push by airlines to fill a greater percentage of seats. Grappling with soaring travel demand, continuing financial problems and record high fuel prices, airlines are filling planes fuller to maximize ticket revenue while holding down operating costs. No. 1

American Airlines filled a record 87 percent of its seats last month, while Delta and Continental filled 85 percent of seats during July. That means many flights were sold out or oversold. Southwest Airlines bumped nearly 32,000 passengers voluntarily or involuntarily in the quarter, more than any other airline.

Source: http://www.usatoday.com/travel/flights/2006-08-03-bumped-usa_t_x.htm

11. *August 03, Federal Computer Week* — **IG notes TWIC security holes.** The Department of Homeland Security needs to address some basic security problems before fully deploying its system for issuing biometric-based identification cards to transportation workers nationwide, according to a report from the department's inspector general (IG). A redacted version of the report (DHS Must Address Significant Security Vulnerabilities Prior To TWIC Implementation), released August 2, states that the Transportation Worker Identification Credential (TWIC) program has significant security vulnerabilities in its systems, documentation and program management. TWIC is currently in its prototype phase. Some of the systems that were evaluated by the IG included enrollment workstations, contractor data center databases and the printers and workstations used to print TWIC cards. IG Report: http://www.dhs.gov/interweb/assetlibrary/OIGr_06_47_Jul06.pdf
Source: <http://www.fcw.com/article95528-08-03-06-Web>

[\[Return to top\]](#)

Postal and Shipping Sector

12. *August 05, Salem-News (OR)* — **Agencies test Oregon post office biohazard detection system.** Biohazard detection equipment and procedures at Salem, OR's main post office were put to the test on Saturday, August 5, during an exercise that focused on the proper response to a biological threat such as anthrax. Several public safety agencies including Salem Fire, Oregon State Police, and the Marion County Health Division conducted the joint exercise with the United States Postal Service. During the exercise, an alarm was activated and postal employees evacuated the facility to a safe location, established a command post, while initiating a call to 911 and completing other emergency notification procedures. Salem Fire's hazardous materials team secured the facility to prevent further contamination and provided decontamination to the postal employees. Oregon State Police provided security.
Source: http://www.salem-news.com/articles/august052006/hazmat_driss_8506.php

13. *August 03, DM News* — **USPS working to keep fuel costs down, speaker says.** The U.S. Postal Service (USPS) is concerned about rising fuel costs and doing everything it can to control these costs, according to a postal official who spoke at the quarterly Mailers' Technical Advisory Committee in Washington, DC, on Wednesday, August 2. "Going forward, expenses are above plan, especially fuel costs and the cost of living increases driven by consumer inflation," said Robert J. Pedersen, acting chief financial officer and executive vice president at the USPS. Pedersen also said as of May 2006, fuel costs have increased 16.7 percent over last year. What's more, the USPS has said that a sharp growth in fuel costs — both for its vehicles and facilities — was a key driver for the recent filing of a rate increase in 2007. "We recently announced two agreements with our competitors who are also suppliers, and there is every effort being made to keep fuel costs as low as we possibly can [when working with them]," Pedersen said. He was referring to the August 1 announcement that USPS has extended its

domestic air transportation of mail agreement with FedEx Express, a subsidiary of FedEx Corp., through 2013. On July 1, USPS began a new extended arrangement with UPS.

Source: <http://www.dmnews.com/cms/dm-news/direct-mail/37734.html>

[\[Return to top\]](#)

Agriculture Sector

- 14. July 27, Associated Press — Plum pox spreads to New York.** The plum pox virus, which decreases fruit production but doesn't harm people, has been detected for the first time in New York at a Niagara County orchard, agriculture officials announced. The virus was found on plum tree leaf samples collected by the state Department of Agriculture and Markets as part of a seven-year survey for the virus. The plum pox virus was detected in neighboring Pennsylvania in 1999 and Canada, within five miles of the Niagara County location, in 2000. The strain found in all three locations, the D strain, is less virulent and easier to contain than other strains, authorities said. Plum pox is a viral disease of stone fruits, including peaches, nectarines, plums and apricots. The virus is spread by insects, in whose mouths the virus can stay viable for about an hour. The U.S. Department of Agriculture, which confirmed the presence of the virus in New York, will work with state officials on an eradication program. Plum pox information: <http://www.apsnet.org/online/feature/PlumPox/>
Source: http://www.yorkdispatch.com/business/ci_4102550

[\[Return to top\]](#)

Food Sector

- 15. August 05, Food Safety and Inspection Service — Tennessee firm recalls ground beef.** Southeastern Meats, a Chattanooga, TN, firm, is voluntarily recalling approximately 4,337 pounds of ground beef that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Saturday, August 5. The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. The ground beef was produced on July 31 and August 1, and was distributed to retail establishments and institutions in Georgia and Tennessee. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_026_2006_Release/index.asp
- 16. August 04, Food Safety and Inspection Service — Texas firm recalls ground beef.** Plains Meat Company, LTD., a Lubbock, TX, firm, is voluntarily recalling approximately 13,078 pounds of ground beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Friday, August 4. The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. The ground beef was produced between July 31 and August 4, 2006 and was sent to restaurants and distributors in Amarillo and Lubbock, TX. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration.

Source: http://www.fsis.usda.gov/News_&_Events/Recall_025_2006_Release/index.asp

17. *August 04, Agence France–Presse* — **Indian state bans soft drinks after Coke, Pepsi get toxic label.** An Indian state has banned the sale of soft drinks as the country's highest court told the U.S. beverage giants Pepsico and Coca–Cola to reveal the ingredients of their products. "The ban will be in force in all educational institutes, including medical and technical colleges and universities and offenders would be punished," a spokesperson from the administration of northern Rajasthan state announced Friday, August 4. He argued that soft drinks producers were required to print statutory warnings on their products. "Manufacturers are required to print 'not only dangerous for human consumption, but also the quantity of the residues, if any, on each label,'" said spokesperson K. Tiwari. The Press Trust of India said the state legislative assembly of the northern state of Punjab also removed soft drinks from the menu of its lawmakers beginning Friday, August 4.

Source: http://news.yahoo.com/s/afp/20060804/hl_afp/indiaushealthpepsi_060804150522:_ylt=Alis8A9hGZp8rVfQuqt8zTSJOrgF:_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

[\[Return to top\]](#)

Water Sector

18. *August 04, Payson Roundup (AZ)* — **Ordinance would make taking water a crime.** The Town of Star Valley, AZ, is looking into an ordinance that would make it illegal for anyone outside the boundaries of the town to draw water from Star Valley. The ordinance reads that water required to meet the requirements of the town Safe Yield Study is not to be allowed to be withdrawn for use outside of the town. It also states that water is necessary to provide for the usual daily operation of the municipality and immediate preservation of the public peace, health, safety and general welfare of the municipality. The ordinance will take effect immediately upon passage.

Source: <http://www.paysonroundup.com/section/localnews/story/24606>

[\[Return to top\]](#)

Public Health Sector

19. *August 06, Agence France–Presse* — **Bangladesh launches polio drive.** More than 700,000 volunteers fanned out across Bangladesh to help vaccinate 24 million children against polio amid signs that the virus has staged a comeback in the country. Bangladesh had been unofficially polio–free since 2000 but a new case was identified in January, prompting authorities to start new vaccination drives, the health ministry said Sunday, August 6. "We've begun the vaccination drive across the country this morning. All of country's 24 million children under the age of five will be vaccinated," health ministry spokesperson Golam Kibria said. "There have been a steady number of new cases since March and we are worried the polio virus is traveling too fast," Kibria said.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: http://news.yahoo.com/s/afp/20060806/hl_afp/healthbangladesh

20. *August 05, Bloomberg* — Thailand reports second human bird flu death in two weeks.

Thailand reported that the bird flu virus had killed a man in a central province, the second such human death in less than two weeks, a senior official at the Health Ministry said Saturday, August 5. A 27-year-old man in Uthai Thani province who died on August 3 tested positive for the H5N1 virus, Thawat Suntrajarn, director general of the ministry's disease control department, said. He was the country's 16th human bird flu death. Thailand, the world's fourth-biggest poultry exporter, has widened its search for avian flu patients and improved surveillance for the virus in poultry after the government on July 26 confirmed a death of a 17-year-old man from bird flu, its first human fatality in seven months.

Source: <http://www.bloomberg.com/apps/news?pid=20601080&sid=aErnC5SxgzE&refer=asia>

21. *August 05, Shanghai Daily (China)* — China orders recall of drug that killed child. The Ministry of Health has banned sales of a popular injectable antibiotic that's been linked to the death of a 6-year-old girl in northern China. In addition to the fatality in Heilongjiang, more than three-dozen other adverse reactions were reported in that province and in Qinghai, Guangxi, Zhejiang and Shandong. Patients receiving the drug, clindamycin phosphate glucose, have complained of symptoms ranging from vomiting and diarrhea to chest and kidney pain. The girl who died received an intravenous injection of the drug to treat a cold on July 24. She developed a high fever 20 minutes later. Liu went into a coma and died three days later. Authorities linked her death and the problems suffered by others to the clindamycin phosphate glucose produced by Anhui Huayuan Worldbest Biology Pharmacy Co, a subsidiary of Shanghai Worldbest Co Ltd.

Source: http://www.shanghaidaily.com/art/2006/08/05/288283/China_ords_recall_of_drug_that_killed_child.htm

22. *August 04, Times of India* — New cases of polio reported in India. Over 85 new cases of polio were reported from across Uttar Pradesh, India, during the past one-and-a-half months, taking the total number of people affected by the disease to 121, a senior official said on Friday, August 4. Director General, Family Welfare, L.B. Prasad said that there is an outbreak of polio in Moradabad and Nagar. In Moradabad alone, 45 polio cases were reported in the past three months, he said. Prasad indicated that the figure may go up in the next few days as the monsoon is conducive to the spread of the virus.

Source: <http://timesofindia.indiatimes.com/articleshow/1855211.cms>

23. *August 03, U.S. Food and Drug Administration* — U.S. Food and Drug Administration developing method to identify hoax bioterror incidents. Researchers at the U.S. Food and Drug Administration (FDA) National Center for Toxicological Research (NCTR) are developing a quick, cost-effective way to screen for and identify bioterror agents and other substances used in hoax incidents. The testing method uses a technology called mass spectrometry. This technique identifies and quantifies compounds, based on the structure and chemical properties of their molecules, quickly and with a very high degree of accuracy. The testing process works in a way similar to the FBI's fingerprint library for criminals. A researcher can take patterns generated by a mass spectrometer's analysis of a substance to be

identified and compare them to a database of known substances, for immediate recognition. Although other testing methods, such as DNA testing, are available, they are costly and involve lengthy processes that can delay by days detection of micro-organisms that can cause disease. This new technique is very fast, taking about seven minutes for each sample on the mass spectrometer following three to eight hours of sample preparation time.

Source: <http://www.fda.gov/bbs/topics/NEWS/2006/NEW01424.html>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

24. *August 04, Associated Press* — Backups to 911 being reviewed. While the Public Service Commission investigates an outage that left much of Wyoming without 911 service for hours Tuesday, August 2, some in law enforcement are questioning the effectiveness of backup systems. Michael Dunne, a spokesperson for Qwest Communications, said the backup plan worked as calls were routed to city lines. But not everyone in law enforcement agreed, noting that some communities were without their 911 service for three to seven hours. In many areas, law enforcement contacted local media, hoping to spread the word that 911 service was down and to tell people they could contact emergency services through other means. But even that caused complications. Dispatchers are trained to take 911 calls before other calls, but with everything coming in on the same lines, there was no way to distinguish one call from another. Dispatchers also had to get callers' phone numbers and locations — information the 911 system provides automatically — over the phone.

Source: <http://www.billingsgazette.net/articles/2006/08/04/news/wyoming/50-backup.txt>

25. *August 03, Mercury News (CA)* — New technologies enhance tornado warning systems. For years, outdoor tornado sirens, the Emergency Broadcast System, and local weather radio, have been the main ways people have learned about nearby emergencies and what to do about them. But advances in technology have created new opportunities to inform people about impending disasters. With text messaging, for example, people can be told not only that a disaster is happening, but also which direction they should go to escape it. Reverse 911 calling systems could call all cell phones within a target area with important information. Targeted messages to Internet addresses could push information to people with broadband access. Many tornado alley counties and states are inching toward new, better integrated hazard alert systems. In Wichita, KS, for example, ever since the city set up its outdoor siren system in the late 1940s, the procedure's been the same: When a tornado warning is in effect, all of the city's roughly 90 sirens sound off. That sort of system creates false alarms and teaches people to ignore warnings, experts warn, so many counties are upgrading to systems that will sound sirens only in areas facing real danger.

Source: http://www.mercurynews.com/mld/mercurynews/news/politics/151_90757.htm

Information Technology and Telecommunications Sector

26. *August 03, Security Focus* — **Mozilla multiple products remote vulnerabilities.** The Mozilla Foundation has released thirteen security advisories specifying vulnerabilities in Mozilla Firefox, SeaMonkey, and Thunderbird. These vulnerabilities allow attackers to: execute arbitrary machine code in the context of the vulnerable application; crash affected applications; run arbitrary script code with elevated privileges; gain access to potentially sensitive information; and carry out cross-domain scripting attacks.
For a list of vulnerable products: <http://www.securityfocus.com/bid/19181/info>
Solution: New versions of Firefox, SeaMonkey, Camino, and Thunderbird are available to address these issues. Most Mozilla applications have self-updating features that may be used to download and install fixes. For information on obtaining and applying fixes: <http://www.securityfocus.com/bid/19181/references>
Source: <http://www.securityfocus.com/bid/19181/discuss>
27. *August 03, Security Focus* — **Microsoft Internet Explorer HHCtrl ActiveX Control memory corruption vulnerability.** Microsoft Internet Explorer is prone to a memory corruption vulnerability. This is related to the handling of the HHCtrl ActiveX Control. Attackers may exploit this issue via a malicious Webpage to execute arbitrary code in the context of the currently logged-in user. Exploitation attempts may lead to a denial-of-service condition as well. Attackers may also employ HTML e-mail to carry out an attack.
For a list of vulnerable products: <http://www.securityfocus.com/bid/18769/info>
Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.
Source: <http://www.securityfocus.com/bid/18769/references>
28. *August 03, Security Focus* — **Microsoft PowerPoint unspecified code execution vulnerability.** Microsoft PowerPoint is prone to an unspecified code-execution vulnerability. A proof-of-concept exploit file designed to trigger this vulnerability has been released. This issue arises when a vulnerable user opens a malicious read-only PowerPoint file and then closes it.
For a list of vulnerable products: <http://www.securityfocus.com/bid/19229/info>
Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.
Source: <http://www.securityfocus.com/bid/19229/references>
29. *August 03, Security Focus* — **Microsoft August advance notification multiple vulnerabilities.** Microsoft has released advance notification that the vendor will be releasing twelve security bulletins for Windows and Office on Tuesday, August 8. The highest severity rating for these issues is 'Critical.'
For a list of vulnerable products: <http://www.securityfocus.com/bid/19331/info>
Source: <http://www.securityfocus.com/bid/19331/discuss>
30. *August 03, CNET News* — **FCC pushes for broadband over power lines.** Federal regulators renewed on Thursday, August 3, their push for a wider rollout of what has been hailed as a viable "third pipe" for the many areas where broadband choices have been limited to digital

subscriber line (DSL) or cable modems. If broadband over power lines, or BPL, takes off, then more Americans, particularly in rural and underserved areas, will be able to plug into high-speed Internet access, and markets dominated by cable and DSL should be forced to lower consumers' bills, members of the Federal Communications Commission (FCC) said at their monthly meeting. The FCC unanimously adopted an order designed to reaffirm and build on the first set of rules issued for the technology in 2004, which had drawn a number of reservations from both inside and outside the industry. The latest order's full text was not immediately released, but a summary version outlines a handful of clarifications (see below). The idea has encountered resistance from amateur radio operators, who complain that BPL could disrupt their systems and those of public safety organizations if deployed without limits. Summary of FCC order: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-266772A1.pdf

Source: http://news.com.com/FCC+pushes+for+broadband+over+power+line/s/2100-1028_3-6101925.html

- 31. August 03, Register (UK) — VoIP hacking exposed.** The latest VoIP security threats and countermeasures were outlined by security experts from SecureLogix and 3Com's Tipping Point at a presentation for the Black Hat security conference in Las Vegas on Wednesday, August 2. SecureLogix CTO Mark Collier and David Endler, director of security research at 3Com, explained how the scope and severity of attacks on Voice over Internet Protocol (VoIP) networks is likely to increase as adoption increases. Alongside the talk, the security researchers released 13 new tools designed to illustrate generic flaws on insecure VoIP systems. These tools, released to assist penetration testers and corporate sys admin, illustrated how it might be possible to overload phones with spurious traffic, flood IP telephony phones with calls, force hang-ups, reboot phones or reassign devices to other users. Source: http://www.channelregister.co.uk/2006/08/03/voip_hacking_exposed/

Internet Alert Dashboard

| Current Port Attacks | |
|---|---|
| Top 10 Target Ports | 1026 (win-rpc), 4672 (eMule), 25 (smtp), 445 (microsoft-ds), 80 (www), 32790 (----), 113 (auth), 6346 (gnutella-svc), 5900 (vnc), 135 (epmap) |
| Source: http://isc.incidents.org/top10.html ; Internet Storm Center | |
| To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov . | |
| Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ . | |

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

- 32. August 05, Associated Press — Evacuations for El Paso; worry over possible dam break.** Forecasters expected more rain Saturday, August 5, in the drenched El Paso area, where a week of storms forced hundreds of people from mountainside neighborhoods and caused flash floods and rocks slides. A new round of evacuations was ordered Friday, August 4, after a downpour

flooded homes and streets around El Paso for the sixth straight day. Crews in Mexico had worked overnight Thursday to reduce water levels at the earthen dam in Mexico, which U.S. Army Corps of Engineers officials said was dangerously close to bursting. The corps had estimated that a break in the aging dam, holding water from the Mexican side of the Rio Grande, could send up to six million gallons into El Paso in as little as three minutes. Mayor John Cook said it would be "like a tidal wave hitting El Paso."

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/05/AR2006080500256.html>

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.